

IN THE CLAIMS:

1-26. (Cancelled)

27. (new) A method for authenticating a data processing system, comprising the steps of:

5 generating first information by a first data processing system and delivering the first information to a second data processing system of a control unit;

10 transmitting first data from the second data processing system to the first data processing system over a data line, the first data being generated by the second data processing system with aid of the first information and additional information contained in the second data processing system;

15 generating second data by the first data processing system depending on the first data and transmitting the second data from the first data processing system to the second data processing system over the data line; and

 generating authentication information for authenticating the second data processing system by the second data processing system with aid of the second data.

20 28. (new) A method according to claim 27 wherein the additional information contains a hardware identifier of the second data processing system.

 29. (new) A method according to claim 28 wherein a check is performed with aid of the second data in order to determine whether the second data processing system contains the hardware identifier.

25 30. (new) A method according to claim 27 wherein the second data contain an expiration date and information based on which access rights of the second data processing system are defined.

31. (new) A method according to claim 30 wherein the access rights are assigned with aid of an authorization level.

32. (new) A method according to claim 27 wherein the second data are transmitted in encrypted form.

5 33. (new) A method according to claim 27 wherein the data line comprises a network connection.

34. (new) A method according to claim 27 wherein the data line comprises a point-to-point connection.

10 35. (new) A method according to claim 27 wherein the second data contain a key.

36. (new) A method according to claim 27 wherein authenticity of the second data processing system is verified by a third data processing system contained in an electrophotographic printing or copying system.

15 37. (new) A method according to claim 27 wherein the first information contains a transaction number.

38. (new) A method according to claim 27 wherein the first information is sent per e-mail or mail.

20 39. (new) A method according to claim 38 wherein the first information that is sent to the first data processing system is entered by way of an input unit of the first data processing system.

40. (new) A method according to claim 27 wherein the second data processing system comprises a control unit, a third data processing system of the printing or copying system verifying authenticity of the second data processing system.

25 41. (new) A method according to claim 27 wherein hardware information of the second data processing system that cannot be modified by

the user is used as a hardware identifier of the second data processing system.

42. (new) A method according to claim 27 wherein the second data are processed with aid of an authentication procedure which generates third information, the third information containing an expiration date and access rights of the second data processing system.

43. (new) A method according to claim 42 wherein the authentication procedure generates the same third data in the processing of several second data of different second data processing systems.

44. (new) A method according to claim 27 wherein verification of authenticity of the second data processing system is performed with aid of a challenge/response procedure.

45. (new) A method according to claim 27 wherein the second data contain a signed certificate.

46. (new) A method according to claim 27 wherein the second data contain a key, and the authentication information contains an authentication code generated with the aid of the key.

47. (new) An arrangement for generating authentication information, comprising:

a first data processing system which generates first information, the first information being delivered to a second data processing system of a control unit;

the second data processing system generating first data with aid of the first information and additional information contained in the second data processing system;

a data line over which first data are transmittable from the first data processing system to the second data processing system;

the second data processing system generating second data depending on the first data;

the second data being transmittable from the second data processing system to the first data processing system over the data line; and

- 5 the second data processing system, with aid of the second data, generating authentication information for authenticating the second data processing system.

48. (new) A method for authenticating a control unit of an electrophotographic printing or copying system, comprising the steps of:

- 10 storing first data in a first data processing system of the control unit;

with aid of the first data, with the first data processing system generating authentication information which are transmitted to a second data processing system of the printing or copying system with aid of authentication data;

- 15 verifying authenticity of the first data processing system by the second data processing system; and

defining method access rights of the first data processing system by the second data processing system with aid of the authentication data.

- 20 49. (new) A method according to claim 48 wherein the first data contain a key or signature.

50. (new) A method according to claim 49 wherein the key comprises a public key or a private key.

- 25 51. (new) A method according to claim 48 wherein the data are transmitted between the first data processing system and the second data processing system with aid of a network connection, the first data processing system serving for remote control, remote servicing, or remote diagnostic

analysis of the printing or copying system and has access at least to control units of the printing or copying system after the verification of authenticity.

52. (new) An arrangement for authenticating a control unit of an electrophotographic printing or copying system, comprising:

5 a first data processing system of the control unit which contains first data;

the first data processing system generating authentication information with aid of the first data;

10 the first data processing system transmitting the authentication information to a second data processing system of the printing or copying system with aid of authentication data;

the second data processing system verifying the authenticity of the first data processing system with aid of the authentication data; and

15 the second data processing system defining access rights of the first data processing system with aid of the authentication data.